Cisco TelePresence EndpointTechnical Handbook

Technical Support Guide

July 2012

Contents

Document revision history

Date	Description
February 2011	- Added T3/T1 Immersive System Information - Update commands for C/EX-series Endpoint
February 2011	- Added T3/TCU Immersive System Information
July 2012	- Added Logs Framework diagrams - Updated Movi/Jabber Video information

Introduction

Each system will be provided with its own User Guide, Quick Reference Guide and if needed, an installation manual. This document is a quick reference handbook for basic troubleshooting to assist with providing an understanding of basic troubleshooting method on Cisco TelePresence Infrastructure Products.

Logs framework diagram symbols

Capture the following log files for the different scenarios:

= Standard *(always attach these logs to the service request)*

= If interworked call *(attach only if the call is interworked)*

= Advanced *(TAC normally request these log)*

Log = Logs from Admin (SSH/Telnet) or the Web Interface

Log = Logs from Root Shell *(these logs can only be captured from root (SSH))*

Information on service request

To ensure Cisco TelePresence TAC to assist technical service request and provide quick resolution, TelePresence TAC require a minimum amount of information for each service request.

When reporting the technical service request, please ensure:

- Describe in detail about problem/issue
- Describe how often the problem occurs
- Describe the latest operation before problem occurs, if any
- Describe in detail, procedure to recreate the problem, if any
- Describe in detail, which steps have already been taken in investigating the problem
- Describe the equipment used and the system serial number (from all sites involved)
- Describe the software version of system (from all sites involved)
- Logs from system including configuration and system status

Terminal software for TelePresence Endpoint

Important: Please start the log capture from all systems involved in the call before calls/conferences are started so we capture all the call setup process and ensures that all output is logged to a file so none is lost.

There is multiple terminal software that may use for retrieving the log from system:

Windows HyperTerminal (Serial, Telnet)

Can be found under: Start Menu – All Programs – Accessories – Communications – HyperTerminal.

The Windows Hyper Terminal supports the Telnet protocol only. Please remember to enable the Capture Text option (menu “Transfer” – “Capture Text”).

TeraTerm

Down load the TeraTerm installation file from http://sourceforge.jp/projects/ttssh2/releases/

Supports multiple Protocols, including Telnet and SSH which are the two relevant protocols for the TelePresenceEndpointportfolio. It will automatic detect serial port if you are using USB to serial converter and option for save log with time stamp.

Putty (Serial, Telnet, SSH)

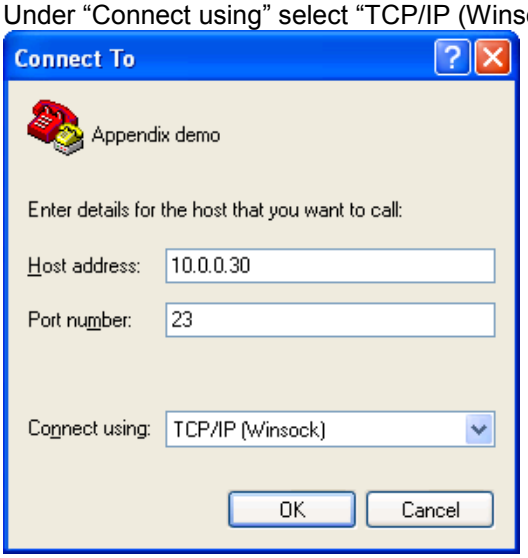
Download the Putty installation file fromhttp://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Supports multiple Protocols, including Telnet and SSH which are the two relevant protocols for the TelePresenceEndpointportfolio.

How to use Windows Hyper Terminal

This following page explains how to use Windows Hyper Terminal.
Please note, Windows Vista and Windows 7 may not have Hyper Terminal installed on default setting.

1. Start HyperTerminal: Start Menu – All Programs – Accessories – Communications – HyperTerminal Supports the Telnet protocol only.
2. Under “Connect using” select “TCP/IP (Winsock)” and enter the System IP address.



3. Default password is cisco, TANDBERG or blank unless changed. Some Endpoint products have “admin” or “root” as login name.

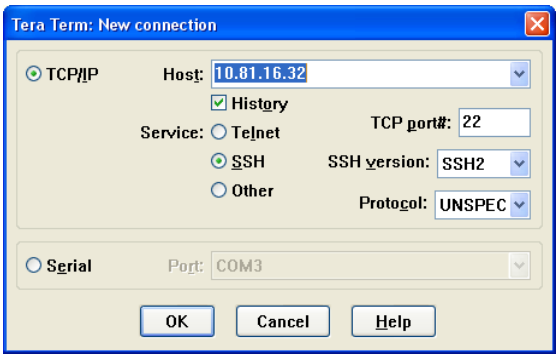
Note: C-series and EX-series Endpoint with TC4.0.0 or newer software, root account is disable by default.

4. To save retrieve logs: Enable the Capture Text option (menu “Transfer” – “Capture Text”), and save it as a *.log file.
5. Type in the respective commands described in Appendix.

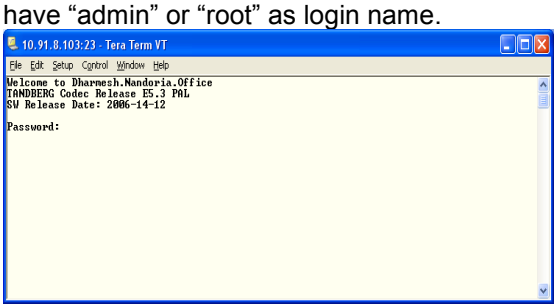
How to use TeraTerm

This following page explains how to useTeraTerm.

1. Start TeraTerm: Start Menu – All Programs – TeraTerm Pro with TTSSH2 – TeraTerm Pro (if install software as default setting).
2. Select “Telnet” and enter the System IP address in “Host”.
   (Or select “SSH” and enter the System IP address in “Host” in order to establish SSH connection between systems.)

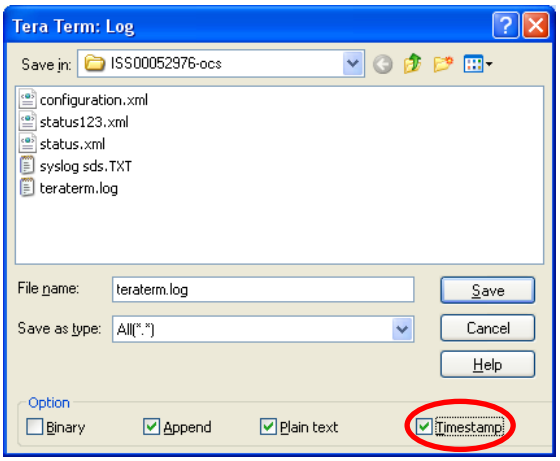


3. Default password is cisco, TANDBERG or blank unless changed. Some Endpoint products have “admin” or “root” as login name.



Note: C-series and EX-series Endpoint with TC4.0.0 or newer software, root account is disable by default.

4. To save retrieve logs: Select “Log” from File menu and select location of saving file and file name. You may check “Timestamp” option which will add timestamp on log base on PC’s clock information.
   (Example of timestamp format on log: [Wed Feb 25 15:10:30 2009]).

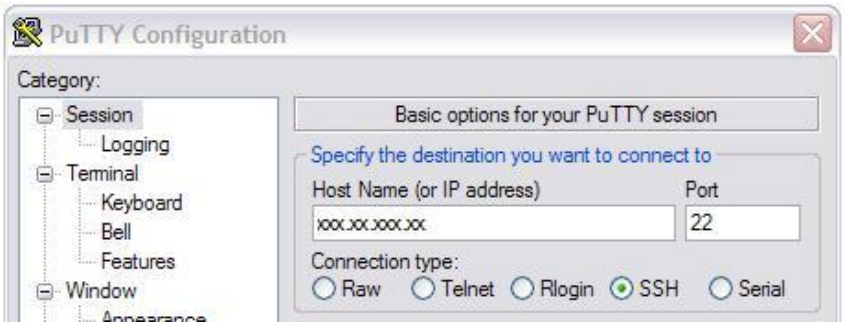


5. Type in the respective commands described in Appendix.

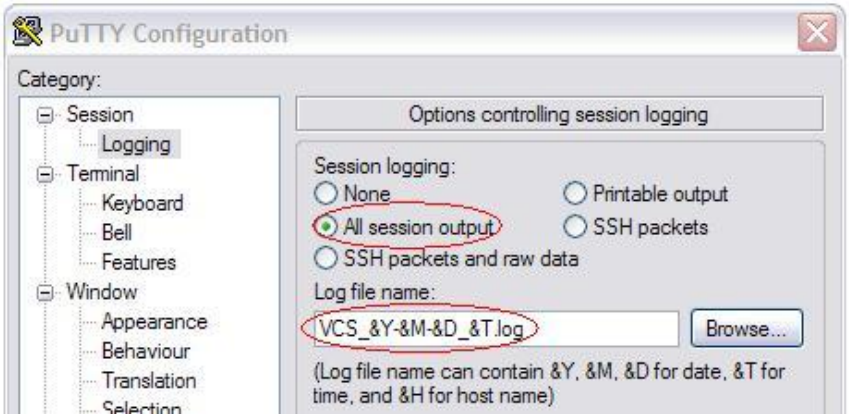
How to use Putty

This following page explains how to use Putty.

1. Start Putty
2. Select “Telnet” and enter the System IP address in “Host Name”.
   (Or select “SSH” and enter the System IP address in “Host Name” in order to establish SSH connection between systems.)



3. Default password is cisco, TANDBERG or blank unless changed. Some Endpoint products have “admin” or “root” as login name.
4. To save retrieve logs: Select “Logging” and choose “All session output” and select location of saving file and file name at “Log file name”.



Note: C-series and EX-series Endpoint with TC4.0.0 or newer software, root account is disable by default.

5. Type in the respective commands described in Appendix.

File transfer software for TelePresence Infrastructure

There are multiple file transfer software applications available, that may be used for retrieving logs from Cisco Telepresence systems and/or uploading files to Cisco Telepresence system. Examples are:

Command Prompt

Can be found under: Start Menu – All Programs – Accessories – Command Prompt. Command Prompt support ftp base file transfer between local PC and TelePresence Infrastructure.

WinSCP

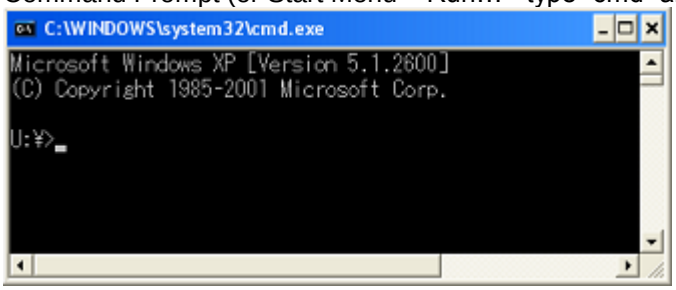
Download the WinSCP installation file from http://winscp.net/eng/index.php

Support SCP protocol with GUI for Windows base PC which use for safely copying of file between local PC and TelePresence Infrastructure.

How to use Windows Command Prompt

This following page explains how to use Command Prompt for ftp.

1. Start Command Prompt HyperTerminal: Start Menu – All Programs – Accessories – Command Prompt (or Start Menu – Run… - type “cmd” and click “ok”)

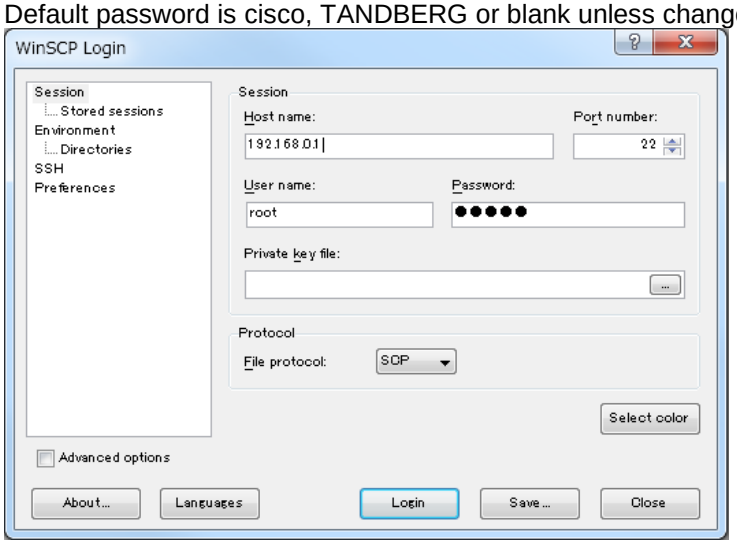


2. Navigate location for saving download file or file folder which to upload to system by using “cd” command.
   For example, save the download log to log folder under C drive on PC, “cd C\log”.
3. Establish ftp connection by using “ftp <ip address>” command.
4. Default password is cisco, TANDBERG or blank unless changed. Some Endpoint products have “admin” or “root” as login name.
5. Basic command which will use on ftp session
   - ls – list the file directory
   - cd <foldername> - navigate to specified directory/folder
   - hash - Toggle printing “#” for each buffer transferred
   - bin – set to binary transfer mode
   - get <filename> – download specified file from codec to PC
   - put <filename> – upload specified file to codec from PC
6. Type “bye” to terminate ftp session between codec and PC

How to use WinSCP

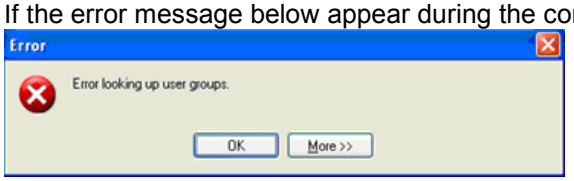
This following page explains how to useWinSCP

1. Start WinSCP: Start Menu – All Programs – WinSCP – WinSCP (if install software as default setting).
2. Select “SCP” as Protocol, enter the System IP address in “Host name”, “root” in “User name” and system password in “Password”.
   Default password is cisco, TANDBERG or blank unless changed.

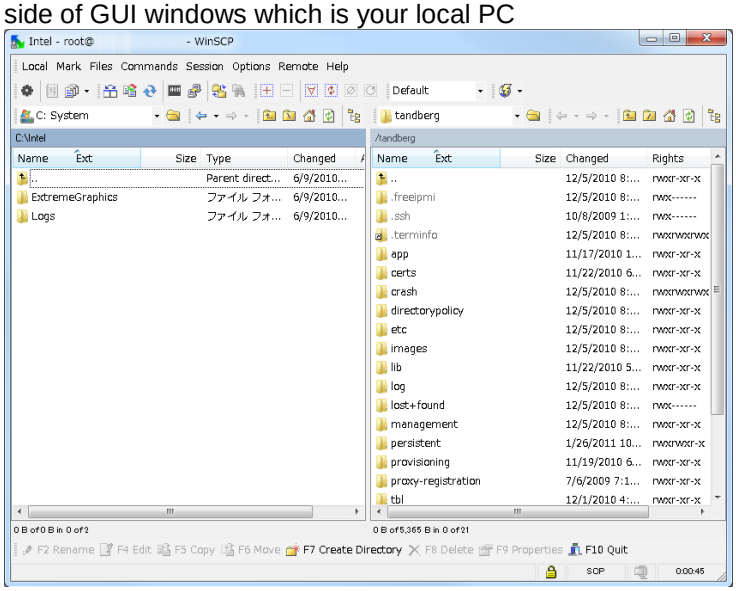


Note: C-series and EX-series Endpoint with TC4.0.0 or newer software, root account is disable by default.

3. After verifying the information click on “Login”.
   If the error message below appear during the connection process, just click “OK” and proceed.



4. Find the log file that would like to retrieve from right side of GUI windows and drag it to left side of GUI windows which is your local PC



Packet Capture software for Cisco TelePresence Infrastructure and Systems

Important: Please start the log capture from all systems involved in the call before calls/conferences are started so we capture all the call setup process and ensures that all output is logged to a file so none is lost.

There are multiple packet capture software that may be used for analyzing communications traffic between Cisco Telepresence systems such as:

Wireshark (IP packet sniffer)

Download the Wireshark installation file from http://www.wireshark.org/download.html

Wireshark is the network protocol analyzer, and is standard across industries.

RS-232 Serial Connection

Most of TelePresence Endpoint has the D-Sub 9 pin data port on the back of the unit that may be used for configuration and administration. The data port may also use for initial configuration. Software upgrades may also be monitored via the serial ports.

Any RS-232 emulation can be used, such as Microsoft HyperTerminal, TeraTerm, etc. The default connectivity parameters are:

Model	Parameter	
Classic Endpoint MXP Endpoint	Baud Rate	9600 bps
	Data Bits	8
	Parity	None
	Stop Bits	1
	Flow Control	None

Model	Parameter	
C-SeriesEndpoint * EX90/EX60 and C20 required special console adapter	Baud Rate	38400 bps
	Data Bits	8
	Parity	None
	Stop Bits	1
	Flow Control	None

Model	Parameter	
E20 Endpoint * required special console adapter	Baud Rate	115200 bps
	Data Bits	8
	Parity	None
	Stop Bits	1
	Flow Control	None

How to capture a log from TelePresence C/EX/SX-series Endpoints

Important: Please start the log capture from all systems involved in the call before calls/conferences are started so we capture all the call setup process and ensure that all output is logged to a file so none is lost.

This chapter explains how to capture the complete log file available for TelePresence C-series and EX-series Components.

The table below lists the commands needed for the TelePresence C-series and EX-series Endpoint. Please type all commands in the same Telnet/SSH session.

All retrieved logs should attach to ticket including a description and compress multiple attachments into one file.

Logs – C-series

The logs in the diagram below should be included on initial support requests for each scenario.

Logs \ Scenario	IP issue (H323)	IP issue (SIP)	Touchpanel issues	Reboot issue	Camera issue
Xstatus					
Xconfiguration					
log.tar.gz (reboot the system first!)					
log ctx H323Packet debug 9					
log ctx SipPacket debug 9					
log ctx camera debug 9					
TCPDUMP					
Tools					
Ping					
netstat -eth0					
netstat -rn					
Other devices					
VCS(s) Xstatus					
VCS(s) Xconfiguration					
VCS(s) diagnostics log (DEBUG)					
VCS(s) diagnostics interworking log (DEBUG)					
VCS(s) TCPDUMP					
Other useful information					
Network diagram					

* For more information, please see the introduction section “Logs framework diagram symbols”

IP issues (H323)

Commands in bold

- Open the console/telnet/ssh session with codec
- Reboot codec by **xCommand boot**
- Reopen the console/telnet/ssh session with codec
- **xstatus**
- **xconfig**
- **log ctx H323Packet debug 9** (TC2.x or prior software version, please use"**log ctx H323Stack debug 9**")
- Make a call and keep running until you have recreated the problem
- **xstatus**, if issue related to video/audio channel status etc.
- Hang up call
- **log ctx H323Packet debug off** (TC2.x or prior software version, please use"**log ctx H323Stack debug off**")
- Once recreated the problem and captured the log, reboot codec by **xCommand boot**
- Access to codec WebGUI for download log file, http://<ipaddress of coded>
- Download the latest file "log.tar.gz"
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

Important: Tracing MUST be turned off when done. It's not recommended to let the tracing stay on when the system is used in production.

IP issue (SIP)

Commands in bold

- Open the console/telnet/ssh session with codec
- Reboot codec by **xCommand boot**
- Reopen the console/telnet/ssh session with codec
- **xstatus**
- **xconfig**
- **log ctx SipPacket debug 9**
- Make a call and keep running until you have recreated the problem
- **xstatus**, if issue related to video/audio channel status etc.
- Hang up call
- **log ctx SipPacket debug off**
- Once recreated the problem and captured the log, reboot codec by **xCommand boot**
- Access to codec WebGUI for download log file, http://<ipaddress of coded>
- Download the latest file "log.tar.gz"
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

Important: Tracing MUST be turned off when done. It's not recommended to let the tracing stay on when the system is used in production.

Reboot Issue

- After codec restart Access to codec WebGUI for download log file, http://<ipaddress of coded>
- Download the latest file "log.tar.gz"
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

Basic network status check from C/EX-series Endpoint

Commands in bold

- Open the console/ssh session with codec and login as "root" user
- **ping <ip address>**, check reachability
- **netstat eth0**, current connected ports on codec
- **netstat -rn**, current network routing on codec

Sniff the packets on C/EX-Series Endpoint

Note: Require TC2.0 or newer software version

Note: This method should only use when request by TelePresence TAC.

Important: This works on both H.323 and SIP call, however encryption must be disabled.
For SIP, make sure not to use TLS for signaling.

Commands in bold

- Open the console/ssh session with codec and login as “root” user
- **tcpdump –n –s 1500 –w /tmp/tcpdump.pcapip and not port 22**
- Make a call and keep running until you have recreated the problem
- **Ctrl + C**
- Open WinSCP and reteieve the sniffer log under /tmp directory.
- Attach file to the ticket – Remember to name these or include a description andcompress multiple attachments into one file

Important: Tracing log MUST delete as tmp folder has limited desk space andnot design to capture log.

Note: Make sure to retrieve sniffer log before restarting codec. Sniffer log saved in /tmp directory will be erased after restart codec.

How to de-activate audio/video protocol in C/EX-series Endpoint

C-series Endpoint support CapSet filter feature useful for connection between legacy system, interop testing, etc.

Sample of CapSet filter commands;

- To force G.722.1 -> disable all other:
  xConfig Experimental CapsetFilter: AAC-LD;G.722;G.711a;G.711mu;G.729AB;G.729;G.729A
- To force H.263 -> disable H.264
  xConfig Experimental CapsetFilter: H.264;H.264RCDO;H.264NIL
- To force H.261 -> disable H.264 and H.263
  xConfig Experimental CapsetFilter: H.264RCDO;H.264NIL;H.263;H.263PP
- To resetCapSet filter
  xConfig Experimental CapsetFilter: ""

Default factory C/EX-series Endpoint

Commands in bold

- Open the console/ssh session with codec and login as “root” user
- **rm /mnt/base/active/config.db**, this remove the current configuration file from Codec
- **reboot**

or

- Open the console/ssh session with codec and login as “admin” user
- **xCommandsystemunitFactoryReset Confirm: Yes**

Note: You may have configuration back up by retrievingconfig.db file. Log in as root using WinSCP, navigate to the folder: ‘/mnt/base/active/’ and copy the file ‘config.db’ to your local PC.

If EX-series Endpoint is not accessible or rebooting use power switch for factory default

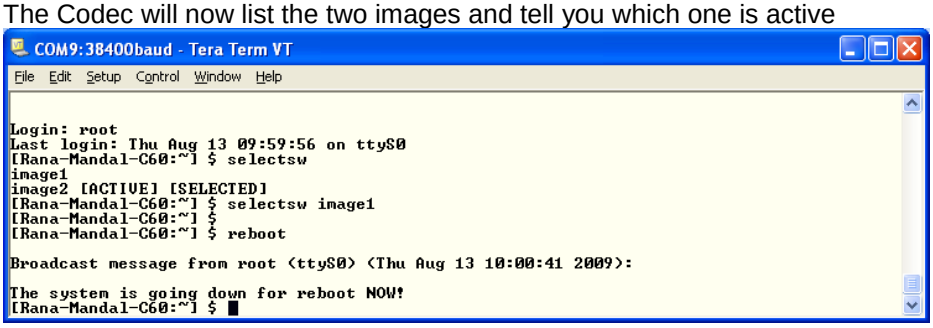
- Unplug power cable
- Re plug power cable
- Immediately when the green led in the bottom left corner of the EX90 lights up, press and hold the power button for 10 seconds (the led will turn off), until the green led lights up again.
- Push the power button twice within two seconds (two short pushes)

Revert back previous software version on C/EX-series Endpoint

Commands in bold

- Login as root, i.e., **ssh root@<ipaddress>**or use ssh terminal software (same method available when connecting Endpoint from console).
- Execute the command**: selectsw**

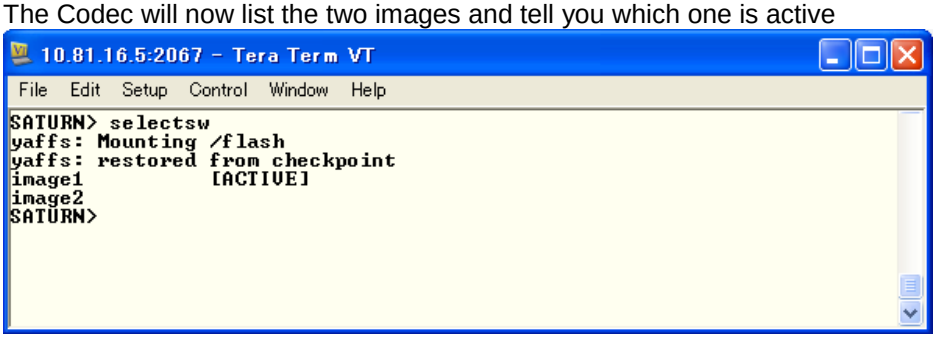
- The Codec will now list the two images and tell you which one is active



- Check feedback and select image: **selectsw image1**(if feedback is “image2 [ACTIVE] [SELECTED]”) or **selectsw image2**(if feedback is “image2 [ACTIVE] [SELECTED]”)
- Reboot the system, **reboot**
- Codec will automatically restart with previous sw version of Codec had

Alternative method for revert back software by changing the boot configuration

- Connect a serial cable to the system at 38400, 8, N, 1
- Reboot the system, and hold **b** until Press 'b' to enter u-boot message appears
- Press **c** to stop auto boot, then SATURN> prompt will return.
- Execute the command: **selectsw**
- The Codec will now list the two images and tell you which one is active

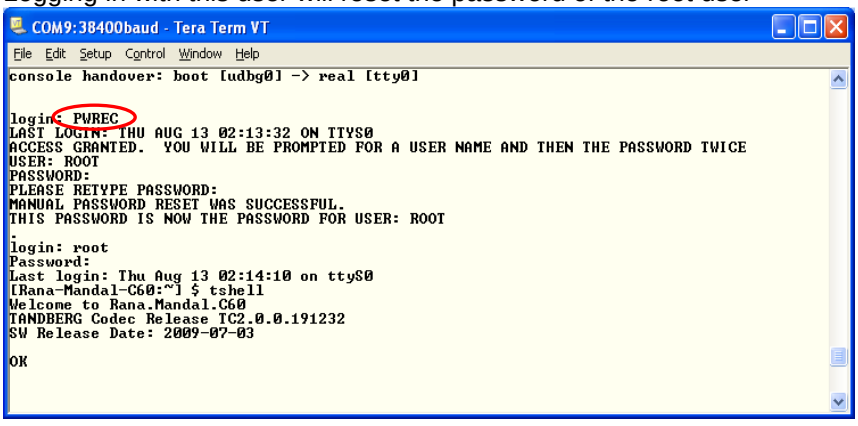


- Check feedback and select image: **selectsw image1**(if feedback is “image2 [ACTIVE] [SELECTED]”) or**selectsw image2** (if feedback is “image2 [ACTIVE] [SELECTED]”)
- Reboot the system, **boot**
- Codec will automatically restart with previous sw version of Codec had

Reset Password on C/EX-Series Endpoint

Commands in bold

- Connect a serial cable to the system at 38400, 8, N, 1
- Reboot the system, power cycle
- Log in with the user **"PWREC".** This user is only available a short period of time after reboot. Logging in with this user will reset the password of the root user



- Change to Endpoint Operation mode, **tsh**
- Set a new admin password, **xCommandSystemUnitAdminPassword SetPassword:<password>**

Monitor diagnostic for RMA

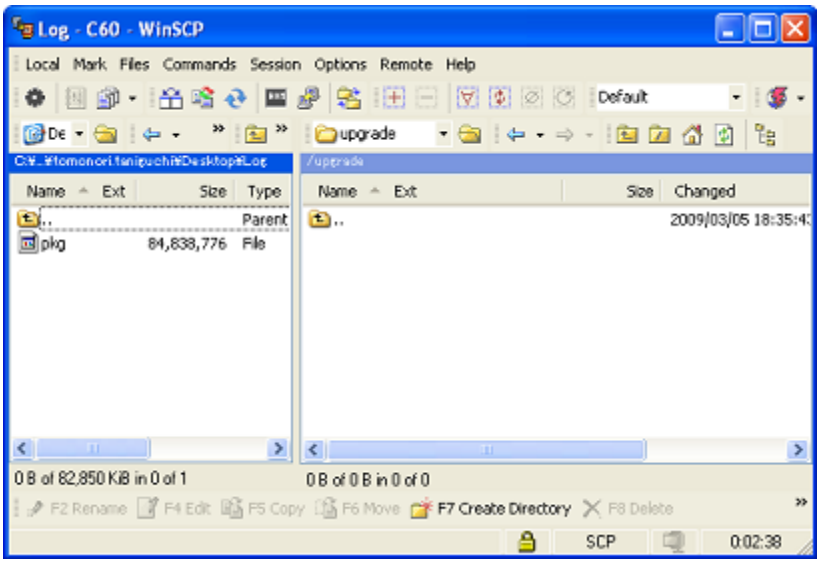
- Please download latest monitor diagnostic tool and reporting template from partner site and follow the manual come together with tool.

How to upgrade TelePresence C/EX-series Endpoint software

This chapter explains how to upgrade C-series and EX-series Endpoint by using SCP software for incase of problem with upgrading software from WebGUI or TMS.

Commands in bold

- If upgrading to a main release, i.e from TC3.x to TC4.x, open a console/ssh session with codec and login as “admin” user and type:
  xCommandSystemUnitReleaseKey Add Key:<releasekey>
- Open WinSCP and establish the connection with codec
- Upload software to /upgrade folder
  Rename file to “pkg..



- Wait for completion of file transfer.
- SW upgrade automatically start after completion of file transfer

How to capture a log from TelePresence T3/T1 Immersive System

Important: Please start the log capture from all systems involved in the call before calls/conferences are started so we capture all the call setup process and ensure that all output is logged to a file so none is lost.

This chapter explains how to capture the complete log file available for TelePresence T3/T1 Immersive System.

All retrieved logs should attach to ticket including a description and compress multiple attachments into one file.

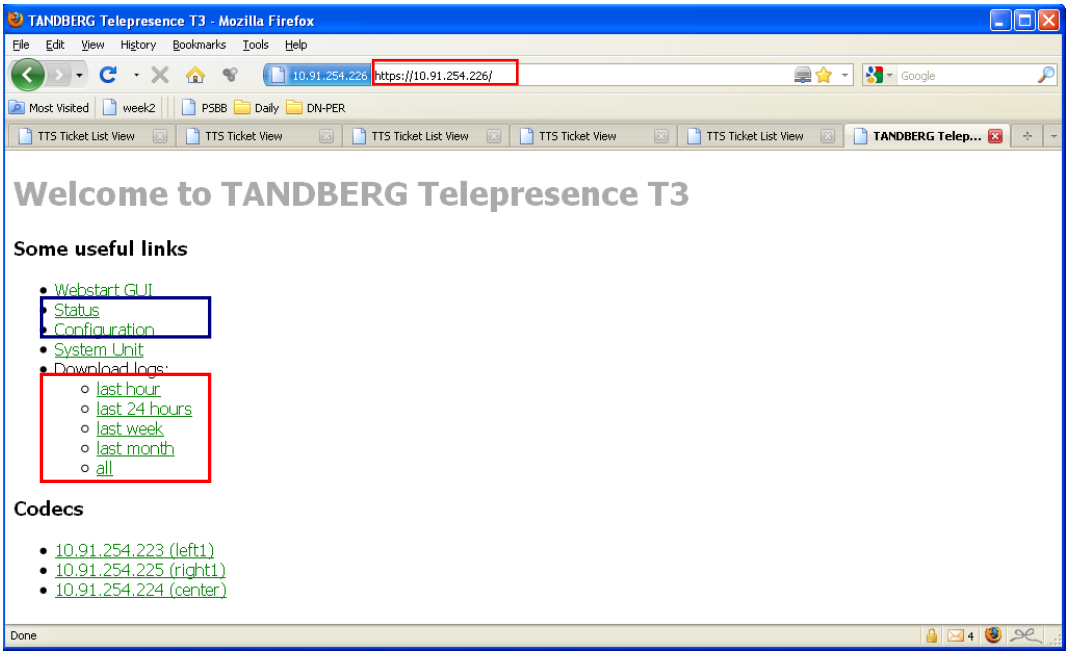
Retrieving Log from each C90 codec in T3/T1 Immersive System

Please refer “How to capture a log from C/EX-series Endpoint” chapter

Retrieving Log from TelePresence Control Unit (TCU)- Using the web GUI (Preffered method)

The TCU logs should be captured for any issue regarding the Cisco TelePresence T3/T1 Immersive system and its various components.

- Access TCU web via HTTPS, select the respective log as per date and time of problem
- User name is admin and no password in default



- Download logs bye selecting a proper time period spanning the time of the issue, but preferably as short as possible.The system configuration and status is included in the downloaded file.
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

Notice that this is the prefered method as the log file will contain the system status and configuration.

Retrieving Log from TelePresence Control Unit (TCU) - Directly from TCU

The TCU logs should be captured for any issue regarding the Cisco TelePresence T3/T1 Immersive system and its various components.

- Connect the keyboard and Mouse to the TCU via the USB ports.
- The logs are stored on the E drive at the following path: **E:/tandberg/logs**. These logs should be saved to a USB thumb drive. The USB thumb drive should be 2 GB or larger. When the drive is inserted into the TCU, it will be seen as the F:/ drive.
- With Keyboard and mouse connected, press the **Ctrl+Shift+Esc** keys to open theTask Manager window.
- Select File, then New Task.
- Type explorer in the field
- Navigate to **E:/tandberg/logs**
- Sort the files by date
- Save all files with the same date as the incident.
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

Revert back previous software version on TCU

- Connect the keyboard and Mouse to the TCU via the USB ports.
- Press **CTRL+ALT+DEL** to restart the TCU
- When TCU is restarting, continue to press the keyboard key **F8**
- You will see a screen , current booting image is high lighted
  option 1 – Windows XP embedded 1
  option 2 – Windows XP embedded 2
- Select other image by up / down arrow.
- TCU will then boot up with the old software

How to upgrade TelePresence T3/T1 Immersive System software

This chapter explains how to upgrade T3/T1 Immersive System by using SCP software.

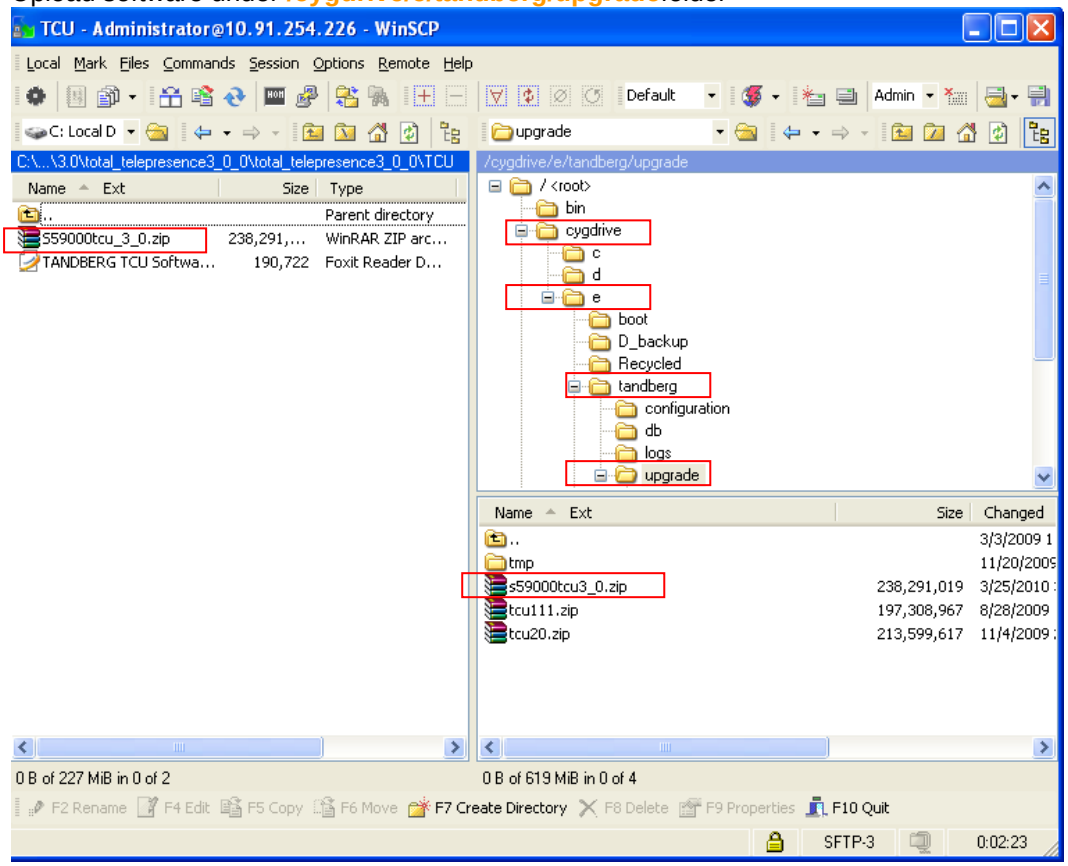
Upgrade C90 codec in T3/T1 Immersive System

Please refer “How to upgrade C/EX-series Endpoint software” chapter

Upgrade TelePresence Control Unit (TCU)– by using SCP software

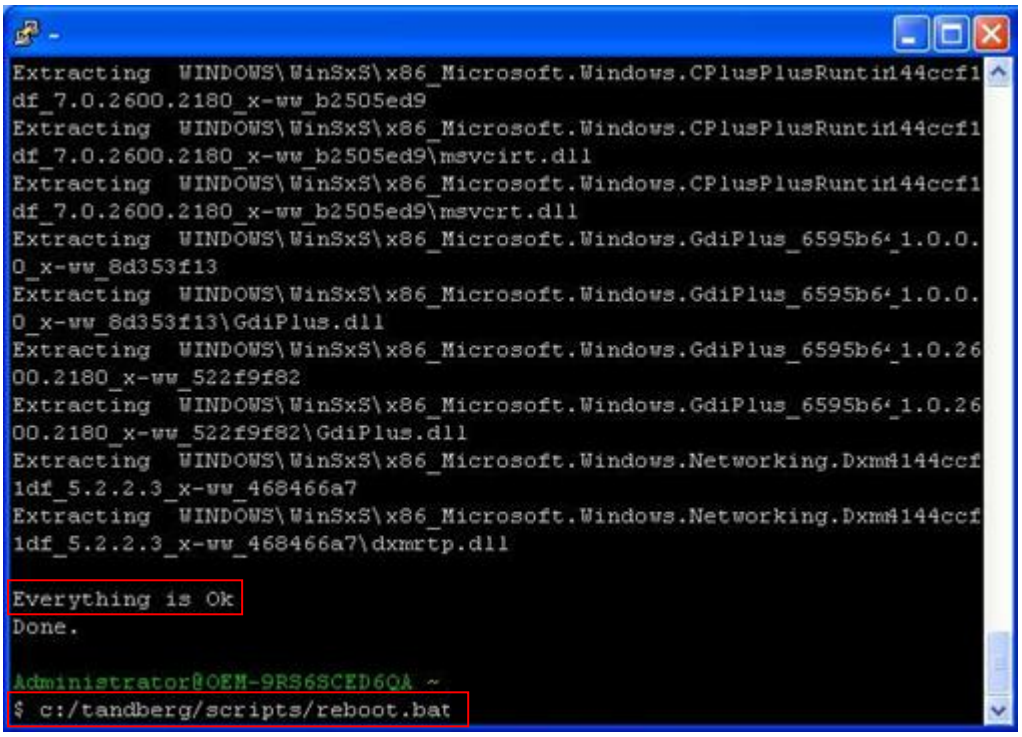
Commands in bold

- Open WinSCP and establish the connection with TCU
- User Name is Administrator and default password istec unless changed.
- Upload software under **/cygdrive/e/tandberg/upgrade**folder



- Wait for completion of file transfer
- Open the ssh session with TCU
- User Name is Administrator and default password istec unless changed.
- Execute software upgrade,**C:/tandberg/scripts/upgrade.sh e:/tandberg/upgrade/<image_name>**
  Image_name = TCU software file name

- Once all upgrade completed successfully, “Everything is ok“message prompt back on SSH console.



- reboot system, **C:/tandberg/scripts/reboot.bat**
- TCU boot up with new software version

Upgrade TelePresence Control Unit (TCU) – by using USB memory stick

Requirement

- 2 GB or larger USB memory stick
- The TCU software image file must be zipped (in this example, refer to it as image.zip)

Preparation - USB memory stick

- Download liveusb-creator software from https://fedorahosted.org/releases/l/i/liveusb-creator/liveusb-creator-2.7.zip (doesn't have to be latest version of liveusb-creator)
- Download Fedora software, Fedora-9-i686-Live-KDE.iso, http://archives.fedoraproject.org/pub/archive/fedora/linux/releases/9/Live/i686/Fedora-9-i686-Live-KDE.iso
- Insert the USB memory stick in the PC
- Format the USB memory stick (FAT1/T32)
- Unzip and start the liveusb-creator software
- Browse for the Fedora ISO image
- Select a Persistent Storage of 500MB (use arrow keys to get the exact size)
- Press **Create Live USB**
- Create a folder named **tandberg** in the root of the USB memory stick
- Put the **image.zip** file into the **tandberg**folder
- Put the update scripts into the **tandberg** folder
- Double click the **image.zip** and open **the tandberg/scripts** folder
- Copy all the files in this folder to the **tandberg** folder on the USB memory stick

Upgrading the TCU software
Commands in bold

- Turn off TCU
- Insert USB memory stick in TCU
- Attached a USB keyboard to the TCU
- Power on TCU
- He BIOS must be set up to boot from USB

- Stop the boot process by pressing **Delete** key
- Change boot order to USB as first order (noted the original boot configuration first)
- Save changes and exit from BIOS setting menu
- Log in as root after system boot up (with Fedora Linux), no password by default
- Execute, **mkdir stick**
- Execute, **mount /dev/sdbl stick**
- Execute, **cd stick/tandberg/**
- Execute, **./setup.sh /dev/sda ./**
- Execute, **cd ..**
- Execute again, **cd ..**
- Remove the USB memory stick
- Turn off TCU by switch off the power
- Power the TCU back on
- Enter BIOS again and change back boot order to original configuration
- Save changes and exit from BIOS setting menu

How to capture a log from TelePresence E20 Endpoint

Important: Please start the log capture from all systems involved in the call before calls/conferences are started so we capture all the call setup process and ensure that all output is logged to a file so none is lost.

This chapter explains how to capture the complete log file available for TelePresence E20 Components.

The table below lists the commands needed for the TelePresence E20 Endpoint. Please type all commands in the same Telnet/SSH session.

All retrieved logs should attach to ticket including a description and compress multiple attachments into one file.

Logs – E20

The logs in the diagram below should be included on initial support requests for each scenario.

Logs \ Scenario	IP issue (H323)	IP issue (SIP)	Reboot issue
Xstatus			
Xconfiguration			
log ctx SipPacket debug 9			
log ctx H323Packet debug 9			
Latest.log			
TCPDUMP			
Tools			
Ping			
Other devices			
VCS(s) Xstatus			
VCS(s) Xconfiguration			
VCS(s) diagnostics log (DEBUG)			
VCS(s) diagnostics interworking log (DEBUG)			
VCS(s) TCPDUMP			
Other useful information			
Network diagram			

* For more information, please see the introduction section “Logs framework diagram symbols”

IP issue (SIP)

Commands in bold

- Open the console/telnet/ssh session with codec
- Reboot codec by **xCommand boot**
- Reopen the console/telnet/ssh session with codec
- **xstatus**
- **xconfig**
- **log ctx SipPacket debug 9**
- Make a call and keep running until you have recreated the problem
- **xstatus**, if issue related to video/audio channel status etc.
- Hang up call
- **log ctx SipPacket debug off**
- Once recreated the problem and captured the log, reboot codec by **xCommand boot**
- Access to codec WebGUI for download log file, http://<ipaddress of coded>
- Click the “logs” tab and download “latest.log” file under Historical log files
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

Important: Tracing MUST be turned off when done. It’s not recommended to let the tracing stay on when the system is used in production.

Reboot Issue

- After codec restart Access to codec WebGUI for download log file, http://<ipaddress of coded>
- Click the “logs” tab and download “Latest. log” file
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

Basic network status check from E20 Endpoint

Commands in bold

- Open the console/ssh session with codec and login as “root” user
- **ping <ip address>**, check reachability
- **netstat eth0**, current connected ports on codec
- **netstat -rn**, current network routing on codec

How to de-activate audio/video protocol in E20 Endpoint

E20 Endpoint support CapSet filter feature useful for connection between legacy system, interop testing, etc.

Sample of CapSet filter commands;

- To force G.722.1 -> disable all other:
  xConfig Experimental CapsetFilter: AAC-LD;G.722;G.711a;G.711mu;G.729AB;G.729;G.729A
- To force H.263 -> disable H.264
  xConfig Experimental CapsetFilter: H.264;H.264RCDO;H.264NIL
- To force H.261 -> disable H.264 and H.263
  xConfig Experimental CapsetFilter: H.264RCDO;H.264NIL;H.263;H.263PP
- To resetCapSet filter
  xConfig Experimental CapsetFilter: ""

Default factory E20 Endpoint

Commands in bold

- Open the console/ssh session with codec and login as “root” user
- **rm /mnt/base/active/config.db**, this remove the current configuration file from Codec
- **reboot**

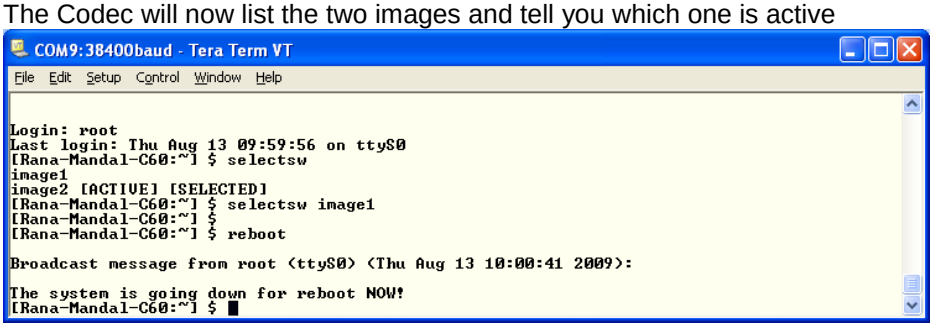
Note: You may have configuration back up by reteieveingconfig.db file. Log in as root using WinSCP, navigate to the folder: ‘/mnt/base/active/’ and copy the file ‘config.db’ to your local PC.

Revert back previous software version on E20 Endpoint

Commands in bold

If you have ssh connection

- Login as root, i.e., **ssh root@<ipaddress>**or use ssh terminal software
- Execute the command**: selectsw**
- The Codec will now list the two images and tell you which one is active



- Check feedback and select image**: selectsw image1**(if feedback is “image2 [ACTIVE] [SELECTED]”) or**selectsw image2**(if feedback is “image2 [ACTIVE] [SELECTED]”)
- Reboot the system, **reboot**
- Codec will automatically restart with previous sw version of Codec had

If you have no remote access connection

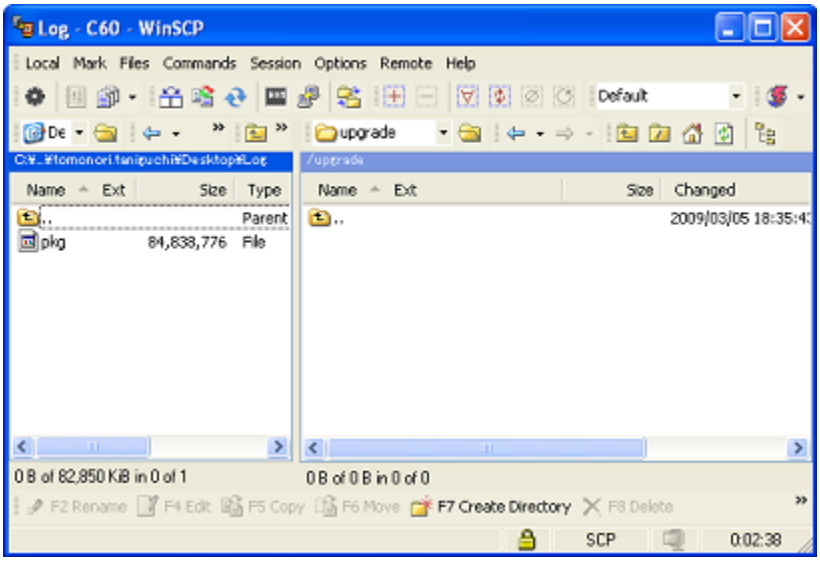
- Hold down the buttons '4' and '6' while plugging in the power cable. Hold until the red status led on top of the E20 start blinking.
- Click the button '4' twice to toggle image (led will blink faster on first click and then solid light at second click)

How to upgrade TelePresence E20 Endpoint software

This chapter explains how to upgrade E20 Endpoint by using SCP software for incase of problem with upgrading software from WebGUI or TMS.

Commands in bold

- Open WinSCP and establish the connection with codec
- Upload software under /upgrade folder
  Note: SW file name should rename to “pkg” before upload it to codec.



- Wait for completion of file transfer.
- SW upgrade automatically start after completion of file transfer
- Wait for completion of software upgrade then open the console/ssh session with codec and login as “admin” user
- reboot system, **xCommand boot**

How to capture a log from MXP series Endpoint

Important: Please start the log capture from all systems involved in the call before calls/conferences are started so we capture all the call setup process and ensure that all output is logged to a file so none is lost.

This chapter explains how to capture the complete log file available for MXP Components.

The table below lists the commands needed for the MXP series Endpoint. Please type all commands in the same Telnet/SSH session.

All retrieved logs should attach to ticket including a description and compress multiple attachments into one file.

Logs – MXP

The logs in the diagram below should be included on initial support requests for each scenario.

Logs \ Scenario	IP issue (H323)	IP issue (SIP)	Reboot issue	ISDN issues
Xstatus				
Xconfiguration				
syslog 3				
syslog 3 | isdn on | dumph221				
Event log				
Serial log				
TCPDUMP				
Tools				
Ping				
Other devices				
VCS(s) Xstatus				
VCS(s) Xconfiguration				
VCS(s) diagnostics log (DEBUG)				
VCS(s) diagnostics interworking log (DEBUG)				
VCS(s) TCPDUMP				
ISDN router				
Other useful information				
Network diagram				

* For more information, please see the introduction section “Logs framework diagram symbols”

IP issues (H323/SIP)

Commands in bold

- Open the console/telnet/ssh session with codec
- **xstatus**
- **xconfig**
- **syslog 3**
- Make a call and keep running until you have recreated the problem
- **xstatus**,if issue related to video/audio channel status etc.
  Don't worry that the screen is scrolling, just type in and press return to retrieve system status log
- Hang up call
- **syslog off**
  Don't worry that the screen is scrolling, just type in and press return to turn off logging

ISDN Issues

Commands in bold

- Open the console/telnet/ssh session with codec
- **xstatus**
- **xconfig**
- **syslog 3**
- **isdn on**
- Make a call and keep running until you have recreated the problem
- **xstatus**, if issue related to video/audio channel status etc.
  Don't worry that the screen is scrolling, just type in and press return to retrieve system status log
- Hang up call
- **syslog off**
  Don't worry that the screen is scrolling, just type in and press return to turn off logging
- **isdn off**
- **dumph221**

Reboot Issue

Commands in bold

- After codec restart open the console/telnet/ssh session with codec
- **eventlog**

  or
- Download event.log file from root directory of Codec
- Open Command prompt (and change home directory, if necessary)
- **ftp <ipaddress>**
- Default password is TANDBERG unless changed. Some Endpoint products have “admin” or “administrator” as login name.
- **hash**
- **bin**
- **get event.log**
- **bye**
- The event. log file transfer to directory of Command Prompt specified.
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

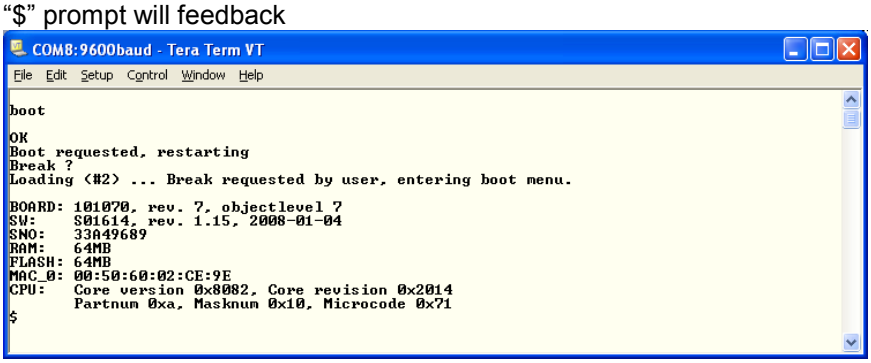
Default factory MXP Endpoint

Commands in bold

- Open the console/telnet/ssh session with codec
- Take backup of system configuration and option keys
- **xCommandDefaultValuesSet Level:3**

  or
- Open the console session with codec by using RS232 cable

- Take backup of system configuration and option keys
- Restart codec and break the boot sequence
- **Ctrl + Break**(for hyper terminal), or **Alt + B** (for TeraTerm/Putty)
- "$" prompt will feedback

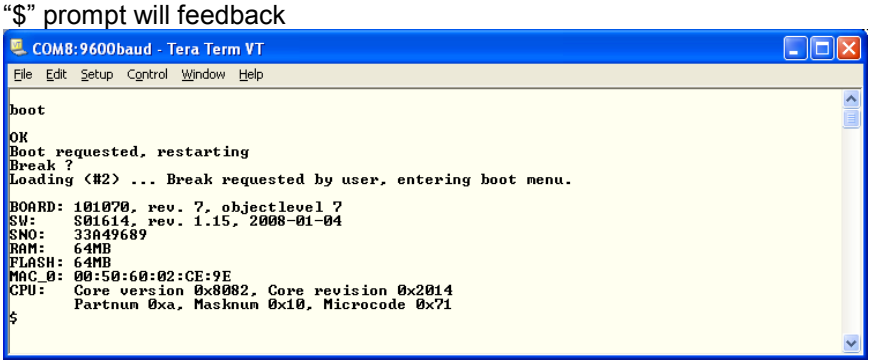


- **eee**
- **q**
- Codec will automatically restart

Revert back previous software version on MXP Endpoint

Commands in bold

- Open the console session with codec by using RS232 cable
- Take backup of system configuration and option keys
- Restart codec and break the boot sequence
- **Ctrl + Break**(for hyper terminal), or **Alt + B** (for TeraTerm/Putty)
- "$" prompt will feedback



- **selectsw**
- Wait for "Active application: x" message
- If x = 1, then **selectsw 2**
- If x = 2, then **selectsw 1**
- **q**
- Codec will automatically restart with previous sw version of Codec had

Monitor diagnostic for RMA

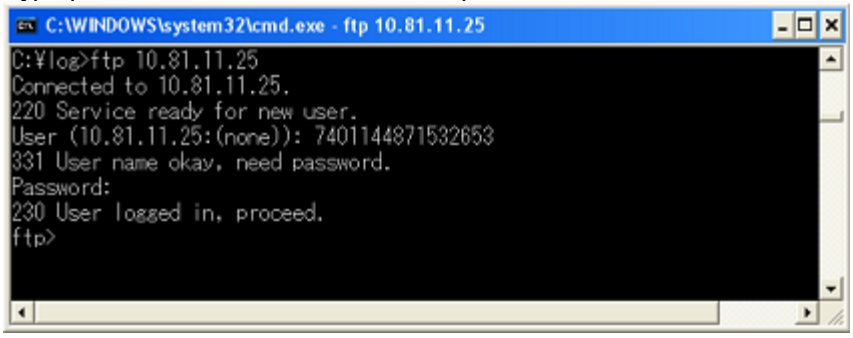
- Please download latest monitor diagnostic tool and reporting template from partner site and follow the manual come together with tool.

How to upgrade MXP series Endpoint software

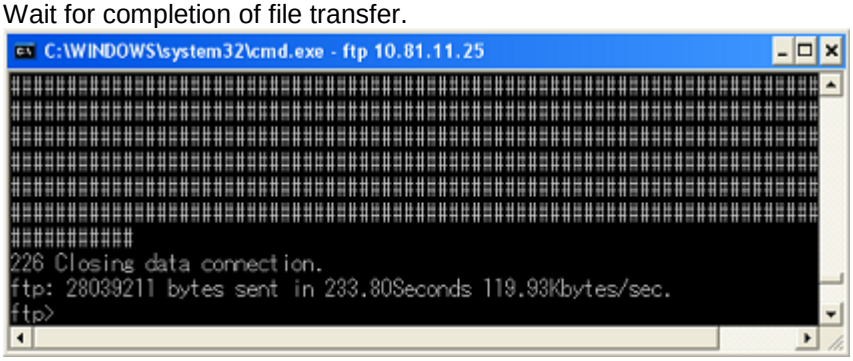
This chapter explains how to upgrade MXP series Endpoint by using ftp software for incase of problem with upgrading software from WebGUI or TMS.

Commands in bold

- Open Command prompt
- Change the directory, if necessary by using “cd” command
  For example, software folder locates under C drive on PC, then **cd C\software**
- **ftp <ipaddress>**
- Type software Release Key in “User:”
- Type password in “Password:”.Default password is TANDBERG unless changed.



- **hash**
- **bin**
- **put <softwarefile>**(or **put <location-of-software\software>**)
  For example, **put s50000f72.pkg**
- Wait for completion of file transfer.



- **bye**
- Reboot the codec manually by remote controller, from Web GUI, from telnet session, etc.

How to capture a log from Classic series Endpoint

Important: Please start the log capture from all systems involved in the call before calls/conferences are started so we capture all the call setup process and ensure that all output is logged to a file so none is lost.

This chapter explains how to capture the complete log file available for Classic Components.

The table below lists the commands needed for the Classicseries Endpoint. Please type all commands in the same Telnet/SSH session.

All retrieved logs should attach to ticket including a description and compress multiple attachments into one file.

IP issues

Commands in bold

- Open the console/telnet session with codec
- **ati1i4i5i6i7i9**
- **dispparam**
- **ipstat**
- **netstat**
- **syslog on**
- Make a call and keep running until you have recreated the problem
- **statin**, if issue related to video/audio channel status etc.
  Don't worry that the screen is scrolling, just type in and press return to retrieve system status log
- **statout**,if issue related to video/audio channel status etc.
  Don't worry that the screen is scrolling, just type in and press return to retrieve system status log
- Hang up call
- **syslog off**
  Don't worry that the screen is scrolling, just type in and press return to turn off logging
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

ISDN Issues

Commands in bold

- Open the console/telnet session with codec
- **ati1i4i5i6i7i9**
- **dispparam**
- **ipstat**
- **netstat**
- **syslog on**
- **isdn on**
- Make a call and keep running until you have recreated the problem
- **statin**,if issue related to video/audio channel status etc.
  Don't worry that the screen is scrolling, just type in and press return to retrieve system status log
- **statout**, if issue related to video/audio channel status etc.
  Don't worry that the screen is scrolling, just type in and press return to retrieve system status log
- Hang up call
- **syslog off**
  Don't worry that the screen is scrolling, just type in and press return to turn off logging
- **isdn off**
- **dumph221**

- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

Reboot Issue

Commands in bold

- After codec restart open the console or telnet session with codec
- **eventlog**

  or

- Download event. log file from root directory of Codec
- Open Command prompt (and change home directory, if necessary)
- **ftp <ipaddress>**
- Default password is TANDBERG unless changed. Some Endpoint products have “admin” or “administrator” as login name.
- **hash**
- **bin**
- **get event.log**
- **bye**
- The event. log file transfer to directory of Command Prompt specified.
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

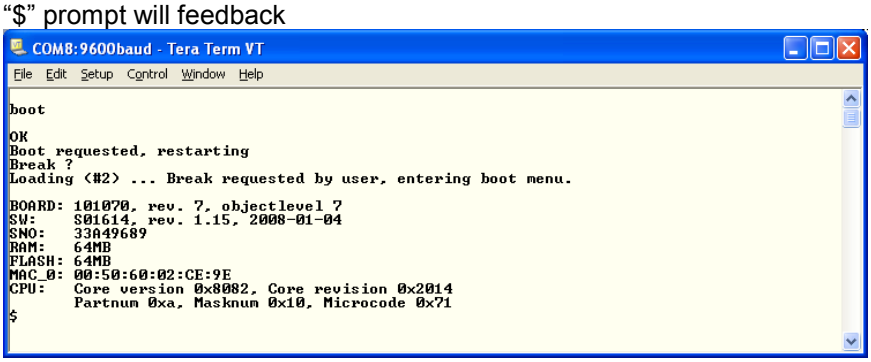
Default factory Classic Endpoint

Commands in bold

- Open the console/telnet/ssh session with codec
- Take backup of system configuration and option keys
- **xCommandDefaultValuesSet Level:3**

  or

- Open the console session with codec by using RS232 cable
- Take backup of system configuration and option keys
- Restart codec and break the boot sequence
- **Ctrl + Break**(for hyper terminal), or **Alt + B** (for TeraTerm/Putty)
- “$” prompt will feedback

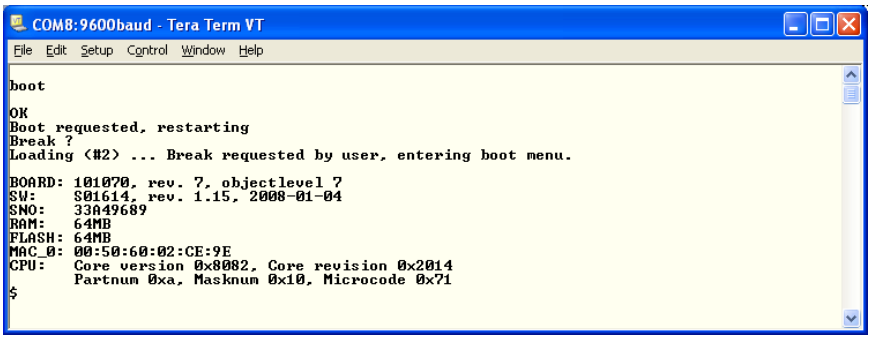


- **eee**
- **q**
- Codec will automatically restart

Revert back previous software version on Classic Endpoint

Commands in bold

- Open the console session with codec by using RS232 cable
- Take backup of system configuration and option keys
- Restart codec and break the boot sequence
- **Ctrl + Break**(for hyper terminal), or **Alt + B** (for TeraTerm/Putty)
- “$” prompt will feedback



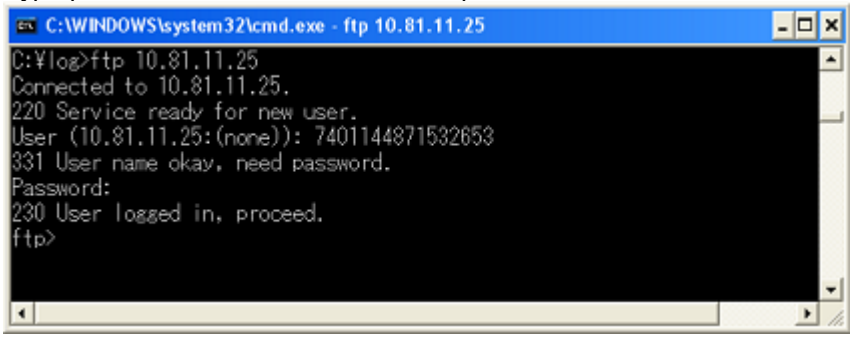
- **selectsw**
- Wait for “Active application: x” message
- If x = 1, then **selectsw 2**
- If x = 2, then **selectsw 1**
- **q**
- Codec will automatically restart with previous sw version of Codec had

How to upgrade Classic series Endpoint software

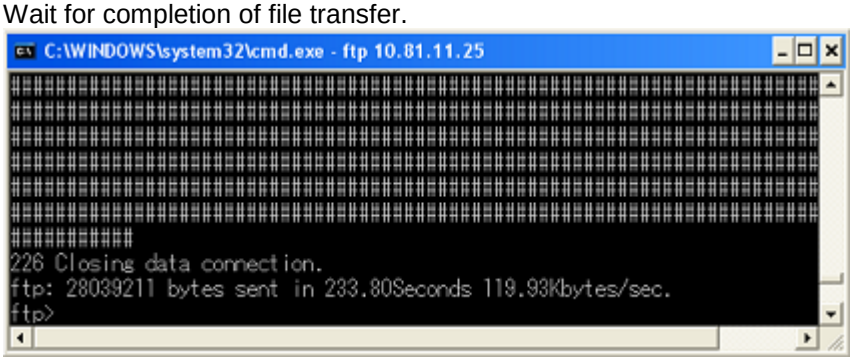
This chapter explains how to upgrade Classic series Endpoint by using ftp software for incase of problem with upgrading software from WebGUI or TMS.

Commands in bold

- Open Command prompt
- Change the directory, if necessary by using “cd” command
  For example, software folder locates under C drive on PC, then **cd C\software**
- **ftp <ipaddress>**
- Type software Release Key in “User:”
- Type password in “Password:”.Default password is TANDBERG unless changed.



- **hash**
- **bin**
- **put <softwarefile>**(or **put <location-of-software\software>**)
  For example, **put s50000f72.pkg**
- Wait for completion of file transfer.



- **bye**
- Reboot the codec manually by remote controller, from Web GUI, from telnet session, etc.

How to capture a log from TelePresence Movi/ Jabber Video

Important: Please start the log capture from all systems involved in the call before calls/conferences are started so we capture all the call setup process and ensure that all output is logged to a file and nothing is lost.

This chapter explains how to capture the complete log file for TelePresence Movi/Jabber Video Components.

The table below lists the commands needed for the TelePresence Movi client.

All retrieved logs should attach to ticket including a description and compress multiple attachments into one file.

Retrieving the Movi/Jabber video logs from PC

Total 6 log files will be generated:

- *Audio.log* Audio specific information
- *Client.log* Information related to the client, GUI & "Business logic"
- *Default.log* Miscellaneous information
- *GStreamer.log* Information from Gstreamer layer
- *TAF.log* The application framework layer information
- *SIP.log* Information about SIP signaling

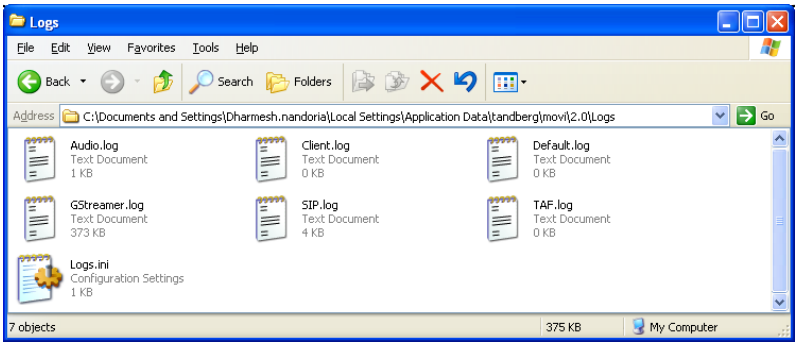
- Open Logs.ini-file and set Level from "WARNING" to "600" (or TRACE)
- Save and restart Movi/Jabber Video
- Reproduce the problem

Log files can be found at the following path:

- <CSIDL_LOCAL_APPDATA>\Cisco\Movi\<major version>.<minor version>\Logs\. (Movi4.0 or prior software version, <CSIDL_LOCAL_APPDATA>\TANDBERG\Movi\<major version>.<minor version>\Logs\.)

  The <CSIDL_LOCAL_APPDATA> folder is typically:

  - On Windows XP:
    %USERPROFILE%\Local Settings\Application Data\
  - On Windows Vista:
    %LOCALAPPDATA% (typically %USERPROFILE%\AppData\Local)



For more detail, please refer "Troubleshooting Movi" section on Cisco TelePresence Movi Administrator Guide

- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file
- Note: for Movi 4.3 and 4.4 (Jabber Video), the default folder would be "JabberVideo" instead of "Movi", e.g.:
  - %USERPROFILE%\AppData\Local\Cisco\JabberVideo\Logs (Windows 7)

Retrieving the Movi/Jabber logs from MAC

Total 6 log files will be generated:

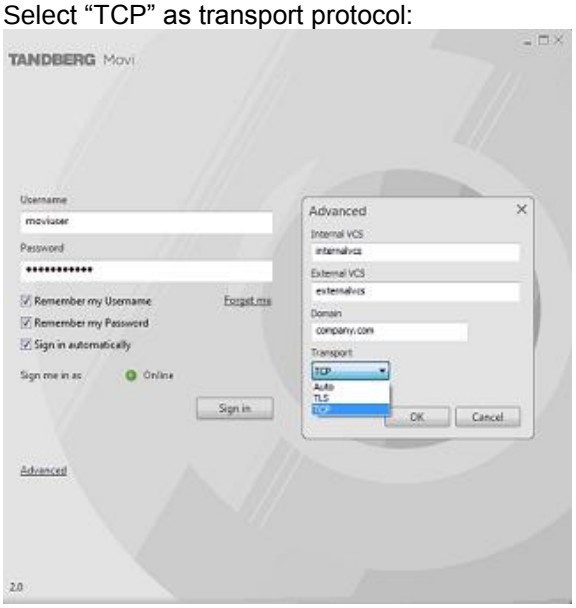
- *Audio.log* Audio specific information
- *Client.log* Information related to the client, GUI & "Business logic"
- *Default.log* Miscellaneous information
- *GStreamer.log* Information from Gstreamer layer
- *TAF.log* The application framework layer information
- *SIP.log* Information about SIP signaling

- Log files can be found at the following path:
  - ~/Library/Logs/Movi

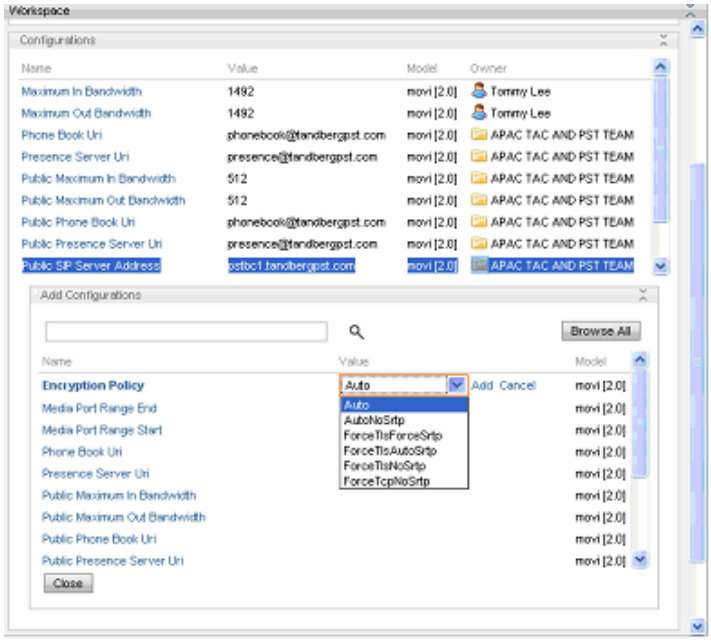
Sniffer the Movi signal and payload from PC - Preparation

Important: The encryption must disable and make sure not to use TLS for signaling.

- If encryption setting in TMS is auto and Advance setting tab is available on Movi client, then encryption can be turned off from client menu.
- Movi 2 client: Go to Advance setting on login menu (Movi 4 doesn't have this! Please see below)
- Select "TCP" as transport protocol:

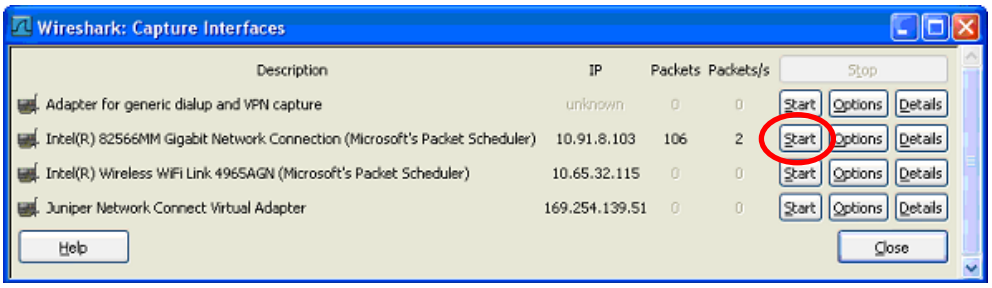


- If Advance option is not available on client then encryption can be turned off using TMS.
- TMS: Go to System – Provisioning, then select either specific group or client
- Change Encryption policy to "**ForceTcpNoSrtp**" (this setting can also be changed locally on your PC; Registry > [HKEY_CURRENT_USER\Software\Cisco\JabberVideo] > EncryptionPolicy



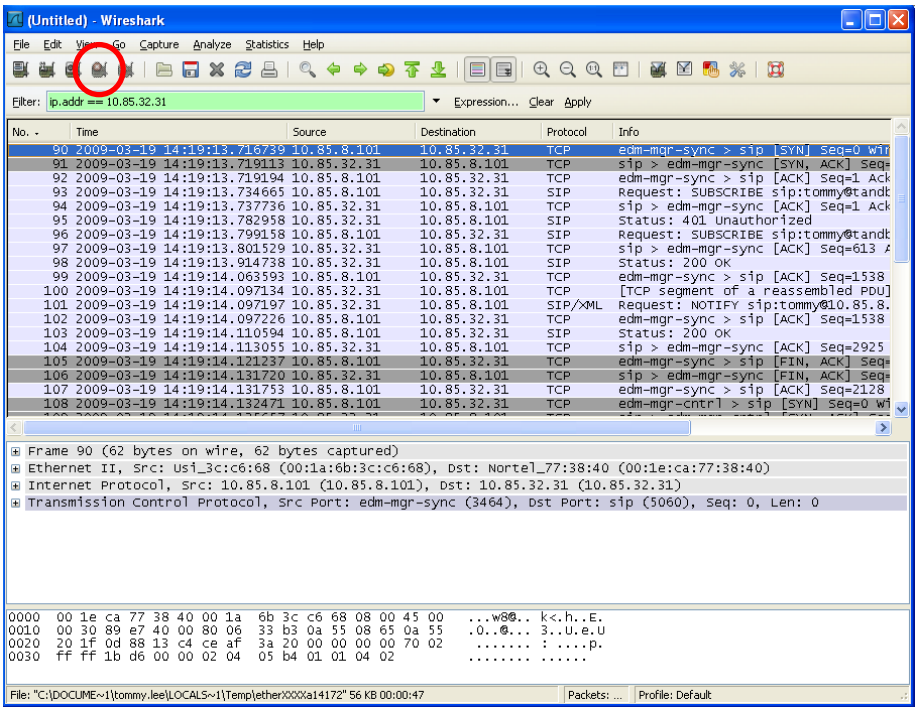
Sniffer the Movi signal and payload from PC

- Start Wire Shark: Start Menu – All Programs – Wire shark
- Select Capture – Interface, from menu
- Click “Start” on interface that PC is using for network connection



Note: If particularly looking for packet between SIP Server (VCS), click “Option”, then type “host <server_ipaddress>” and click “Start”. Only traffic between SIP Server sniffer and file will remain minimum size

- Login the Movi 2 client
- Make a call and keep running until you have recreated the problem
- Stop the sniffer from either Stop Icon on menu or select Capture – Stop, from menu



- Save the retrieved packet (packet range should select “All packets”)
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file